10/067,740
2/8/02
Junichi HAYASHI

(translation of the front page of the priority document of Japanese Patent Application No. 2001-034057)

JAPAN PATENT OFFICE

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: February 9, 2001

Application Number : Patent Application 2001-034057

[ST.10/C] : [JP 2001-034057]

Applicant(s) : Canon Kabushiki Kaisha

March 1, 2002

Commissioner,

Japan Patent Office Kouzo OIKAWA

Certification Number 2002-3012178

CFM 2513 US

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: 2001年 2月 9日

出願番号
Application Number: 特願2001-034057

[ST.10/C]: [JP2001-034057]

出願人
Applicant(s): キヤノン株式会社

2002年 3月 1日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号 出証特2002-3012178

【書類名】　特許願
【整理番号】　4345005
【提出日】　平成13年 2月 9日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 7/00
【発明の名称】　情報処理装置及びその制御方法及びコンピュータプログラム及び記憶媒体
【請求項の数】　21
【発明者】
【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
【氏名】　林　淳一
【特許出願人】
【識別番号】　000001007
【氏名又は名称】　キヤノン株式会社
【代理人】
【識別番号】　100076428
【弁理士】
【氏名又は名称】　大塚　康徳
【電話番号】　03-5276-3241
【選任した代理人】
【識別番号】　100115071
【弁理士】
【氏名又は名称】　大塚　康弘
【電話番号】　03-5276-3241
【手数料の表示】
【予納台帳番号】　003458
【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0001010

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報処理装置及びその制御方法及びコンピュータプログラム及び記憶媒体

【特許請求の範囲】

【請求項１】　ディジタル情報に認証情報を付加する情報処理装置であって、

付加されるディジタル情報に基づいて認証情報を生成する手段と、

生成された認証情報を、前記ディジタル情報に対し、当該ディジタル情報が復元可能に電子透かし情報として埋め込む電子透かし埋め込み手段と

を備えることを特徴とする情報処理装置。

【請求項２】　前記認証情報はディジタル署名であることを特徴とする請求項１に記載の情報処理装置。

【請求項３】　更に、前記ディジタル情報を秘密鍵を用いて暗号化する暗号化手段を有し、前記ディジタル署名は前記ディジタル情報を前記秘密鍵で暗号化したデータであることを特徴とする請求項１又は２に記載の情報処理装置。

【請求項４】　更に、前記ディジタル情報のハッシュ値を算出するハッシュ値計算手段と、前記ハッシュ値を秘密鍵を用いて暗号化する暗号化手段を有し、前記ディジタル署名は前記ディジタル情報のハッシュ値を前記秘密鍵で暗号化したデータであることを特徴とする請求項１または２に記載の情報処理装置。

【請求項５】　前記認証情報は、ＭＡＣであることを特徴とする請求項１に記載の情報処理装置。

【請求項６】　更に、前記ディジタル情報のハッシュ値を算出するハッシュ値計算手段と、前記ハッシュ値を秘密鍵を用いて演算する演算手段を有し、前記ＭＡＣは前記ディジタル情報のハッシュ値を前記秘密鍵を用いて演算したデータであることを特徴とする請求項５に記載の情報処理装置。

【請求項７】　認証情報は、前記ディジタル署名に加えて、更に、日付情報、位置情報、時間情報、装置の固有情報、署名者の固有情報のうち少なくとも一つを含むことを特徴とする請求項２に記載の情報処理装置。

【請求項８】　認証情報が電子透かしとして埋め込まれたディジタル情報を

認証する情報処理装置であって、

前記ディジタル情報から電子透かしとして埋め込まれている認証情報を第１の認証情報として抽出する手段と、

抽出された認証情報を電子透かしとして前記ディジタル情報から除去し、仮オリジナルディジタル情報に復元する電子透かし除去手段と、

該電子透かし除去手段で電子透かしを除去するこで復元された仮オリジナルディジタル情報に基づき、第２の認証情報を生成する生成手段と、

前記第１の認証情報と前記第２の認証情報を比較する比較手段と

を備えることを特徴とする情報処理装置。

【請求項９】　前記第１の認証情報と前記第２の認証情報が等しい時には前記入力されたディジタル情報は改ざんされていない、等しくない場合には改ざんされているとして報知する報知手段とを備えることを特徴とする請求項８に記載の情報処理装置。

【請求項１０】　前記認証情報はディジタル署名であることを特徴とする請求項８に記載の情報処理装置。

【請求項１１】　更に、前記ディジタル署名を公開鍵を用いて復号する復号手段を有し、前記比較手段は、前記第２の認証情報を復号した情報と前記第１の認証情報とを比較することを特徴とする請求項８に記載の情報処理装置。

【請求項１２】　更に、前記電子透かしが除去されたディジタル情報のハッシュ値を算出するハッシュ値計算手段と、前記ディジタル署名を公開鍵を用いて復号する復号手段を有し、前記認証手段は、前記第２の認証情報を前記公開鍵で復号した情報と前記ハッシュ値とを比較することを特徴とする請求項８に記載の情報処理装置。

【請求項１３】　前記認証情報はＭＡＣであることを特徴とする請求項８に記載の情報処理装置。

【請求項１４】　更に、前記電子透かしが除去されたディジタル情報のハッシュ値を算出するハッシュ値計算手段と、前記ＭＡＣを秘密鍵を用いて演算する演算手段を有し、前記認証手段は、前記ＭＡＣを前記秘密鍵で復号した情報と前記ハッシュ値を比較することを特徴とする請求項１２に記載の情報処理装置。

【請求項１５】　認証情報は、前記ディジタル署名、且つ／或いは、ＭＡＣに加えて、更に、日付情報、位置情報、時間情報、装置の固有情報、署名者の固有情報のうち少なくとも一つを含むことを特徴とする請求項８に記載の情報処理装置。

【請求項１６】　ディジタル情報に認証情報を付加する情報処理装置の制御方法であって、

付加されるディジタル情報に基づいて認証情報を生成する工程と、

生成された認証情報を、前記ディジタル情報に対し、当該ディジタル情報が復元可能に電子透かし情報として埋め込む電子透かし埋め込み工程と

を備えることを特徴とする情報処理装置の制御方法。

【請求項１７】　認証情報が電子透かしとして埋め込まれたディジタル情報を認証する情報処理装置の制御方法であって、

前記ディジタル情報から電子透かしとして埋め込まれている認証情報を第１の認証情報として抽出する工程と、

抽出された認証情報を電子透かしとして前記ディジタル情報から除去し、仮オリジナルディジタル情報に復元する電子透かし除去工程と、

該電子透かし除去工程で電子透かしを除去するこで復元された仮オリジナルディジタル情報に基づき、第２の認証情報を生成する生成工程と、

前記第１の認証情報と前記第２の認証情報を比較する比較工程と

を備えることを特徴とする情報処理装置の制御方法。

【請求項１８】　コンピュータが読み込み実行することで、ディジタル情報に認証情報を付加する情報処理装置として機能するプログラムであって、

付加されるディジタル情報に基づいて認証情報を生成する工程のプログラムコードと、

生成された認証情報を、前記ディジタル情報に対し、当該ディジタル情報が復元可能に電子透かし情報として埋め込む電子透かし埋め込み工程のプログラムコードと

を備えることを特徴とするコンピュータプログラム。

【請求項１９】　請求項１８に記載のコンピュータプログラムを格納するこ

とを特徴とする記憶媒体。

【請求項２０】　コンピュータが読み込み実行することで、認証情報が電子透かしとして埋め込まれたディジタル情報を認証する情報処理装置として機能するプログラムであって、

前記ディジタル情報から電子透かしとして埋め込まれている認証情報を第１の認証情報として抽出する工程のプログラムコードと、

抽出された認証情報を電子透かしとして前記ディジタル情報から除去し、仮オリジナルディジタル情報に復元する電子透かし除去工程のプログラムコードと、

該電子透かし除去工程で電子透かしを除去するこで復元された仮オリジナルディジタル情報に基づき、第２の認証情報を生成する生成工程のプログラムコードと、

前記第１の認証情報と前記第２の認証情報を比較する比較工程のプログラムコードと

を備えることを特徴とするコンピュータプログラム。

【請求項２１】　請求項２０に記載のコンピュータプログラムを格納することを特徴とする記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ディジタル情報の署名、及び認証をする情報処理方法及び装置と記憶媒体に関するものである。

【０００２】

【従来の技術】

近年、コンピュータとそのネットワークの急速な発達及び普及により、文字データ、画像データ、音声データなど、多種の情報がディジタル化されている。ディジタル情報は、経年変化などによる劣化がなく、いつまでも完全な状態で保存できる一方で、容易に編集・加工を施すことが可能である。こうしたディジタルデータの編集・加工は利用者にとって有益であることが多い。

【０００３】

しかしその一方で、例えば、事故処理で証拠写真を扱う保険会社や、建築現場の進捗状況の記録を扱う建設会社においてはディジタルデータの信頼性は従来のアナログデータと比較して低く、証拠としての能力に乏しいという問題を抱えている。

【０００４】

そこでディジタルデータの改ざん、偽造が行われていた場合にそれを検出するような映像入力装置、システムが提案されてきた。

【０００５】

例えばディジタル署名を利用するシステムは、前記改ざん、偽造を検出するシステムとしてよく知られている。ここでディジタル署名について簡単に説明する。

【０００６】

ディジタル署名とは、送信者がデータと一緒に該データに対応する署名データを送り、受信者がその署名データを検証して該データの正当性を確認することである。ディジタル署名データ生成にハッシュ(Hash)関数と公開鍵暗号を用いたデータの正当性の確認は以下のようになる。

【０００７】

秘密鍵をＫｓ、公開鍵をＫｐとすると、発信者は、平文データＭをハッシュ関数により圧縮して一定長の出力ｈ（例えば１２８ビット）を算出する演算を行う。次に秘密鍵Ｋｓでｈを変換してディジタル署名データｓを作成する演算、すなわちＤ(Ｋｓ,h) =ｓを行う。その後、該ディジタル署名データｓと平文データＭとを送信する。

【０００８】

一方受信者は受信したディジタル署名データｓを公開鍵Ｋｐで変換する演算、すなわちＥ(Ｋｐ,ｓ)= Ｅ(Ｋｐ,Ｄ(Ｋｓ,h''))= h''と、受信した平文データＭ'を発信者と同じハッシュ関数により圧縮してh' を算出する演算を行い、h'とh''が一致した場合、受信したデータM'が正当であると判断する。

【０００９】

平文データＭが送受信間で改ざんされた場合にはＥ(Ｋｐ,ｓ)= Ｅ(Ｋｐ,Ｄ(Ｋ

ｓ，ｈ’’))＝ｈｈ’’と、受信した平文データＭ’を発信者と同じハッシュ関数により圧縮したｈ’が一致しないので改ざんを検出できるわけである。

【００１０】

ここで、平文データＭの改ざんに合わせてディジタル署名データｓの改ざんも行われてしまうと改ざんの検出ができなくなる。しかし、これはｈから平文データＭを求める必要があり、このような計算はハッシュ関数の一方向性により不可能である。以上、説明したように、公開鍵暗号方式とハッシュ関数を用いたディジタル署名によって、正しくデータの認証を行うことが可能である。

【００１１】

次にハッシュ関数について説明する。ハッシュ関数は上記ディジタル署名の生成を高速化するため等に用いられる。ハッシュ関数は任意の長さの平文データＭに処理を行い、一定の長さの出力ｈを出す機能を持つ。ここで、出力ｈを平文データＭのハッシュ値（またはメッセージダイジェスト、ディジタル指紋）という。ハッシュ関数に要求される性質として、一方向性と衝突耐性が要求される。一方向性とはｈを与えた時、ｈ＝Ｈ(Ｍ)となる平文データＭの算出が計算量的に困難であることである。衝突耐性とは平文データＭを与えた時、Ｈ(Ｍ)＝Ｈ(Ｍ’)となる平文データＭ’(Ｍ≠Ｍ’)の算出が計算量的に困難であること、及び、Ｈ(Ｍ)＝Ｈ(Ｍ’)かつＭ≠Ｍ’となる平文データＭ,Ｍ’の算出が計算量的に困難であることである。

【００１２】

ハッシュ関数としてはMD-2,MD-4,MD-5,SHA-1,RIPEMD-128,RIPEMD-160等が知られており、これらのアルゴリズムは一般に公開されている。

【００１３】

続いて公開鍵暗号について説明する。公開鍵暗号は暗号鍵と復号鍵が異なり、暗号鍵を公開、復号鍵を秘密に保持する暗号方式である。公開鍵暗号の特徴としては、

(a) 暗号鍵と復号鍵とが異なり暗号鍵を公開できるため、暗号鍵を秘密に配送する必要がなく、鍵配送が容易である。

(b) 各利用者の暗号鍵は公開されているので、利用者は各自の復号鍵のみ秘密に

記憶しておけばよい。

(c) 送られてきた通信文の送信者が偽者でないこと及びその通信文が改ざんされていないことを受信者が確認するための認証機能を実現できる。

が挙げられる。

【００１４】

例えば、平文データMに対して、公開の暗号鍵Ｋｐを用いた暗号化操作をＥ(Ｋｐ,M) とし、秘密の復号鍵Ｋｓを用いた復号操作をＤ(Ｋｓ,M) とすると、公開鍵暗号アルゴリズムは、まず次の２つの条件を満たす。

(1) Ｋｐが与えられたとき、Ｅ(Ｋｐ,M) の計算は容易である。Ｋｓが与えられたとき、Ｄ(Ｋｓ,M) の計算は容易である。

(2) もしＫｓを知らないなら、ＫｐとＥの計算手順と、Ｃ＝Ｅ(Ｋｐ,M) を知っていても、Mを決定することは計算量の点で困難である。

【００１５】

次に、上記(1)、(2)に加えて、次の(3)の条件が成立することにより秘密通信が実現できる。

(3) 全ての平文データMに対し、Ｅ(Ｋｐ,M) が定義でき、Ｄ(Ｋｓ,Ｅ(Ｋｐ,M))＝Mが成立する。つまり、Ｋｐは公開されているため誰もがＥ(Ｋｐ,M) を計算することができるが、Ｄ(Ｋｓ,Ｅ(Ｋｐ,M)) を計算してMを得ることができるのは秘密鍵Ｋｓを持っている本人だけである。一方、上記(1)、(2)に加えて、次の(4)の条件が成立することにより認証通信が実現できる。

(4) すべての平文データMに対し、Ｄ(Ｋｓ,M) が定義でき、Ｅ(Ｋｐ,Ｄ(Ｋｓ,M))＝Mが成立する。つまり、Ｄ(Ｋｓ,M) を計算できるのは秘密鍵Ｋｓを持っている本人のみであり、他の人が偽の秘密鍵Ｋｓ'を用いて Ｄ(Ｋｓ',M) を計算しＫｓを持っている本人になりすましたとしても、Ｅ(Ｋｐ,Ｄ(Ｋｓ',M))≠M なので受信者は受けとった情報が不正なものであることを確認できる。また、Ｄ(Ｋｓ,M) が改ざんされても Ｅ(Ｋｐ,Ｄ(Ｋｓ,M)')≠M となり、受信者は受けとった情報が不正なものであることを確認できる。

【００１６】

上記の秘密通信と認証通信とを行うことができる代表例としてRSA暗号やR暗号

やW暗号等が知られている。

【００１７】

ここで、現在最も使用されているRSA暗号の暗号化、復号は次式で示される。

暗号化：暗号化鍵（ｅ，ｎ）　暗号化変換$C=M^{e}(\mathrm{mod}\ n)$

復号：復号鍵（ｄ，ｎ）　復号変換$M=C^{d}(\mathrm{mod}\ n)$

$n=p\cdot q$　　ここでｐ、ｑ　は大きな異なる素数である。

【００１８】

上記のように、ＲｓＡ暗号は暗号化にも復号にもべき乗演算と剰余演算が必要であるので、ＤＥＳをはじめとする共通鍵暗号と比較すると演算量が膨大なものとなり高速な処理は難しい。

【００１９】

以上説明したように、従来技術における改ざん、及び偽造の検出は、ディジタルデータに加えて、前記ディジタル署名を必要とする方式である。通常、ディジタル署名は、ディジタルデータのヘッダ部分などに添付する方式で送信することが行われる。しかしながら、ディジタルデータのフォーマット変換などによって添付されたディジタル署名は容易に除去される可能性がある。ディジタル署名が除去された場合、ディジタルデータの認証をすることはできない。

【００２０】

これを解決した方法が、特開平１０－１６４５４９号公報に示されている。特開平１０－１６４５４９公報においては、ディジタル情報をふたつの領域に分割し、分割された第１の領域からディジタル署名を生成し、生成されたディジタル署名を、分割された第２の領域に電子透かしとして埋め込むことにより、署名が施されたディジタル情報を生成する。一方、認証装置においては、署名が施されたディジタル情報を前記第１の領域と第２の領域に分割し、前記第１の領域から第１のディジタル署名を生成し、第２の領域から電子透かしとして埋め込まれている第２のディジタル署名を抽出する。そして第１のディジタル署名と第２のディジタル署名が等しい時に前記ディジタル情報が改ざん、及び偽造されていないことを認証する方法である。

【００２１】

【発明が解決しようとする課題】

以上説明したように、ディジタルデータの認証をするためには、認証情報をディジタル情報と不可分の状態にしておくことが重要である。前記特開平１０－１６４５４９号公報の方法においては、オリジナルの画像の認証をするために、電子透かしとして署名情報を埋め込んでおり、更にこの電子透かしは除去することが不可能であるため、オリジナルの画像を得ることは出来ない。アプリケーションや利用者によっては、電子透かしの埋め込み自体を「改ざん」であると判断する可能性もある。

【００２２】

【課題を解決するための手段】

本発明はかかる問題点に鑑みなされたものであり、認証情報をディジタル情報と不可分にししつつ、改ざんがなされているか否かを判断でき、しかも改ざんがない限りはオリジナルのディジタル情報に復元することを可能ならしめる情報処理装置及びその制御方法及びコンピュータプログラム及び記憶媒体を提供しようとするものである。

【００２３】

かかる本発明の課題を解決するため、例えば本発明における、認証情報を付加する側の情報処理装置は以下の構成を備える。すなわち、

ディジタル情報に認証情報を付加する情報処理装置であって、

付加されるディジタル情報に基づいて認証情報を生成する手段と、

生成された認証情報を、前記ディジタル情報に対し、当該ディジタル情報が復元可能に電子透かし情報として埋め込む電子透かし埋め込み手段とを備える。

また、認証する側の装置である情報処理装置は以下の構成を備える。すなわち

認証情報が電子透かしとして埋め込まれたディジタル情報を認証する情報処理装置であって、

前記ディジタル情報から電子透かしとして埋め込まれている認証情報を第１の認証情報として抽出する手段と、

抽出された認証情報を電子透かしとして前記ディジタル情報から除去し、仮オリジナルディジタル情報に復元する電子透かし除去手段と、

該電子透かし除去手段で電子透かしを除去するこで復元された仮オリジナルディジタル情報に基づき、第２の認証情報を生成する生成手段と、

前記第１の認証情報と前記第２の認証情報を比較する比較手段とを備える。

【００２４】

【発明の実施の形態】

以下、添付図面に従って本発明に係る実施形態を詳細に説明する。

【００２５】

以下では、情報に認証情報を埋め込む装置として署名装置、その情報を受けて認証する装置を認証装置として説明する。

【００２６】

＜署名装置＞

本実施形態におる署名装置を図２を用いて説明する。

【００２７】

図２において、２０１は画像入力部、２０２はハッシュ値計算部、２０３は暗号部、２０４は電子透かし埋め込み部、２０５は画像出力部である。

【００２８】

まず、画像入力部２０１に対して画像信号がラスタースキャン順に入力される。画像入力部２０１の入力対象としては、イメージスキャナ、画像が記憶された記憶媒体、遠隔から通信によって受信する通信手段等のいずれでも構わない。以降の説明では画像信号はモノクロの多値画像を表現しているが、カラー画像等、複数の色成分を有する画像であるならば、ＲＧＢ各色成分、或いは、輝度、色度成分を上記単色成分として処理すれば良い。

【００２９】

さて、入力された画像信号Ｉは、ハッシュ値計算部２０２、及び電子透かし埋め込み部２０４に出力される。

【００３０】

ハッシュ値計算部２０２は、入力された画像信号Ｉのハッシュ値Ｈを計算して

出力するものである。ハッシュ値Ｈを算出するためにハッシュ関数が用いられるが、本発明においてハッシュ関数は特に限定されることなく、一般に公開されているＭＤ－２、ＭＤ－４，ＭＤ－５，ＳＨＡ－１，ＰＩＰＥＭＤ－１２８，ＲＩＰＥＭＤ－１６０など種々の方式を用いることが可能である。算出されたハッシュ値Ｈは暗号部２０３に出力される。

【００３１】

暗号部２０３は、入力されたハッシュ値Ｈを秘密鍵Ｓを用いて暗号化して出力するものである。本発明において暗号化をするための暗号アルゴリズムは特に限定されることなく、例えば公開鍵暗号であるＲＳＡ暗号などを用いることが可能である。暗号化されたハッシュ値Ｅｓ（Ｈ）は電子透かし埋め込み部２０４に出力される。

【００３２】

電子透かし埋め込み部２０４は、入力された画像信号Ｉに前記暗号化されたハッシュ値Ｅｓ（Ｈ）を可逆の電子透かしとして埋め込み出力する（可逆の電子透かしの詳細な説明は後述する）。電子透かしが埋め込まれた画像信号ｗＩは、画像出力部２０５に出力される。出力対象は、記憶媒体、通信回線等で構わないし、その対象は特に限定されない。

【００３３】

＜認証装置＞

次に、本実施形態における認証装置について図３を用いて説明する。

【００３４】

図３において、３０１は画像入力部、３０２は電子透かし抽出部、３０３は復号部、３０４はハッシュ値計算部、３０５は比較部である。

【００３５】

まず、画像入力部２０１に対して画像信号ｗＩ’がラスタースキャン順で入力される。入力された画像ｗＩ’は電子透かし抽出部３０２に出力される。ここでｗＩ’とは、望ましくは図２に示した署名装置の出力ｗＩに等しいものであるが、改ざん、及び偽造されている場合をも想定して、ここではｗＩ’と表現している。

【００３６】

電子透かし抽出部３０２は、入力された画像信号ｗI'から埋め込まれている電子透かしE's（H）を抽出し、更に可逆の電子透かしを除去するものである。抽出された電子透かしE's（H）、及び電子透かしが除去された画像データI'が出力される。

【００３７】

ここで、ｗI'がｗIに等しい場合には、電子透かしとしてＥｓ（H）が抽出される（即ち、Ｅｓ（H）＝E's（H）である）。更に、この場合には可逆の電子透かしは完全に除去され、画像データＩが出力される（即ち、Ｉ＝Ｉ'である）。一方で、ｗＩ'がｗＩとは異なる場合には、電子透かしとしてＥｓ（H）とは異なるデータが出力される（即ち、Ｅｓ（H）≠E's（H）である）。更に、この場合には可逆の電子透かしは完全に除去されない（即ち、Ｉ≠Ｉ'である）。

【００３８】

更に、電子透かし抽出部３０２は、入力された画像データに電子透かしが埋め込まれているか否かを検出する機能を有する。この機能を用いて、ｗI'としてディジタル署名が電子透かしとして埋め込まれていない画像データが入力された場合には、電子透かし抽出部は、「情報なし」と出力し、その後の認証処理を実行しない。この場合、モニタなどを用いて、「画像データが認証できない」という表示を出力することも可能である。

【００３９】

以上の様に抽出された電子透かしE's（H）は復号部３０３に出力され、電子透かしが除去された画像データＩ'はハッシュ値計算部３０４に出力される。

【００４０】

復号部３０３は、入力されたデータE's（H）を復号して出力するものである。復号に際しては、署名装置において用いられた秘密鍵ｓに対応する公開鍵ｐが用いられる。復号されたデータは比較部３０５に出力される。

【００４１】

ハッシュ値計算部３０４は、入力された画像データＩ'のハッシュ値H'を計算して出力するものである。ハッシュ値を算出するためのハッシュ関数としては、

前記署名装置で用いられたものに等しいハッシュ関数が用いられる。算出されたハッシュ値H'は比較部３０５に出力される。

【００４２】

比較部３０５は、入力されたハッシュ値HとH'を比較することにより、ｗＩ'が改ざん、或いは偽造されたものかどうかを検証するものである。ここで、HとH'が等しい場合にはｗＩ＝ｗＩ'であり、即ち改ざん、或いは偽造されたものではないと判断する。一方で、HとH'が異なる場合にはｗＩ≠ｗＩ'であり、即ち改ざん、或いは偽造されたものと判断する。この場合、その旨を例えば表示装置に表示する。

【００４３】

＜電子透かし埋め込み部＞

次に本実施形態における電子透かし埋め込み部２０４の詳細について説明する。実施形態における、電子透かし埋め込み部で行う処理を簡単に説明すると、電子透かし埋め込み前の画像データにまで完全に復活することができるように、情報を埋め込むものである。

【００４４】

図４は電子透かし埋め込み部２０４の内部構成を示した図である。以下、同図に従って処理の流れを説明する。

【００４５】

画像データＩは電子透かし埋め込み部２０４に入力され、画像データＩに埋め込む電子透かしの埋め込み位置が、埋め込み位置決定部４０１で決定される。次に画像データＩは付加情報埋め込み部４０２に入力され、付加される情報Ｅｓ（Ｈ）に従って、前段の埋め込み位置決定部４０１で決定された位置に電子透かしが埋め込まれる。

【００４６】

そのため、埋め込み位置決定部４０１は、入力された画像データＩ、画像中に付加情報Ｅｓ（Ｈ）を埋め込む位置を表すデータ（各領域を特定する座標と大きさ）を付加情報埋め込み部４０２に出力する。

【００４７】

付加情報埋め込み部４０２には、上記画像データＩに加えて、付加情報Ｅｓ（Ｈ）（複数のビット情報）を入力する。この付加情報Ｅｓ（Ｈ）は、画像データＩにおける上記決定された埋め込み位置に、電子透かし技術を用いて埋め込まれる。この電子透かしの技術を用いた付加情報Ｅｓ（Ｈ）の埋め込みについては後述する。付加情報埋め込み部４０２からは付加情報Ｅｓ（Ｈ）が埋め込まれた電子透かし埋め込みデータｗＩが出力されることになる。

【００４８】

なお、本実施形態では、電子透かし埋め込み装置に入力するデータは、説明を簡単にするため、１画素が８ビット階調（２５６階調）を持つグレースケール画像データであるとする。しかし、入力されるデータは、カラー画像データであっても構わない。カラー画像が入力される場合には、カラー画像の１チャネルの画素値、またはカラー画像の輝度値などを用いることで、同様の埋め込みを行うことが可能である。

【００４９】

また、音声データが入力される場合には、画像の二次元の位置情報を、時間の１次元の情報に置き換えて考えればよく、同様の手法で実現することが可能である。また、動画データが入力される場合には、２次元画像が複数、時間軸に並べられていると解釈することが出来るため、各２次元画像を同様の手法で処理することにより、基本的に、適用可能である。従って、カラー画像、音声、動画に電子透かしの埋め込みを行う場合も、本発明の範疇に含まれる。

【００５０】

次に、本実施形態における、電子透かし埋め込み、電子透かし分離（抽出）の基本原理について説明する。

【００５１】

＜パッチワーク法＞

本実施形態では付加情報Inf（上記実施形態でのＥｓ（Ｈ）が対応する）の埋め込みの為にパッチワーク法と呼ばれる原理を用いている。パッチワーク法については、論文「電子透かしを支えるデータ・ハイディング技術（上）」Walter Bender,Daniel Gruhl,森本典繁,Anthony Lu/日経エレクトロニクス 1997.2.24な

どにも開示されている。そこで、まずパッチワーク法の原理を説明する。

【００５２】

パッチワーク法では画像に対して統計的偏りを生じさせることによって付加情報Ｅｓ（Ｈ）の埋め込みを実現している。

【００５３】

図５を用いて、パッチワーク法の原理を説明する。同図において、原画像から２つの部分集合ＡとＢを選択する。今、部分集合Ａは部分集合a_i５０１に代表される複数の部分集合からなり、部分集合Ｂは部分集合b_i５０２に代表される複数の部分集合からなるとする。

【００５４】

この２つの部分集合は互いに重ならならなければ、本実施の形態におけるパッチワーク法による付加情報Infの埋め込みが実行可能である。

【００５５】

今、部分集合Ａ，Ｂはそれぞれ、Ａ＝｛$a_1, a_2, .., a_N$｝、Ｂ＝｛$b_1, b_2, .., b_N$｝で表されるＮ個の要素からなる集合であるとする。部分集合Ａと部分集合Ｂの各要素a_i，b_iは画素値を持つ画素または画素の集合を表しているとする。

【００５６】

ここで、次の指標ｄを次のように定義する。

$$d = 1/N \cdot \Sigma (a_i - b_i)$$

ここで、Σはｉ＝１～Ｎに関する和である。

【００５７】

これは、２つの集合の画素値の差の期待値を示している。

【００５８】

一般的な自然画像に対して、適当な部分集合Ａと部分集合Ｂを選択し、指標ｄを定義すると、Ｎは十分大きな値の場合には、

$$d \fallingdotseq 0$$

となる性質がある。以降では、このｄを信頼度距離と呼ぶ。

【００５９】

一方で、付加情報Ｅｓ（Ｈ）を構成する各ビットの埋め込み操作として、例えば“１”のビット情報を埋め込む場合、

$a'_i = a_i + c$

$b'_i = b_i - c$

という操作を行う。これは部分集合Ａの全ての要素の画素値に対して「ｃ」を加え、部分集合Ｂの全ての要素の画素値に対して「ｃ」を減ずるという操作である。なお、本実施形態では、以降、この「ｃ」の値を“埋め込み深さ”と呼ぶ。

【００６０】

ここで、先程の場合と同様に、付加情報Ｅｓ（Ｈ）が埋め込まれた画像から部分集合Ａと部分集合Ｂを選択し、指標ｄを計算すると、次の通りになる（各Σはｉ＝１～Ｎの総和である）。

$$d = 1/N \cdot \Sigma (a_i - b_i)$$
$$= 1/N \cdot \Sigma \{ (a_i + c) - (b_i - c) \}$$
$$= 1/N \cdot \Sigma \{ (ai - bi) + 2c \}$$
$$\fallingdotseq 2c$$

つまり、０から一定距離離れた値となる。

【００６１】

他方のビット情報（“０”のビット情報）を埋め込む場合には、

$a'_i = a_i - c$

$b'_i = b_i + c$

の操作を行う。すると、信頼度距離ｄは、

$$d = 1/N \cdot \Sigma (a_i - b_i)$$
$$= 1/N \cdot \Sigma \{ (a_i - c) - (b_i + c) \}$$
$$= 1/N \cdot \Sigma \{ (ai - bi) - 2c \}$$
$$\fallingdotseq -2c$$

となり、０から負の方向へ一定距離はなれた値となる。

【００６２】

即ち、ある画像が与えられた場合に、画像に対して信頼度距離ｄを算出することにより、付加情報が埋め込まれているかを判断することができる。

【００６３】

信頼度距離d≒０ならば付加情報Ｅｓ（Ｈ）は埋め込まれておらず、信頼度距離dが０から一定量以上離れた正の値であるなら、１のビット情報が埋め込まれており、dが０から一定量以上離れた負の値であるなら、０のビット情報が埋め込まれていると判断できることを意味する。

【００６４】

本実施形態では、上記パッチワーク法の原理を応用し、１つの画像に複数のビットの情報を埋め込む。

【００６５】

本実施形態では、１つの画像の互いに異なる領域に、部分集合ＡとＢの組み合わせだけでなく、部分集合Ａ’とＢ’、部分集合Ａ’’とＢ’’、…という複数の組み合わせを想定することで、複数のビットからなる付加情報Ｅｓ（Ｈ）を埋め込む。ただし、部分集合ＡとＢ、部分集合Ａ’とＢ’、部分集合Ａ’’とＢ’’、…の配置は、お互いに重なり合わないことが必要である。

【００６６】

ここで、複数のビット情報が埋め込まれたデータから、ビット情報を抽出する方法について考えてみる。

【００６７】

図６の６０１は、電子透かしが埋め込まれていないデータから計算される信頼度距離ｄの分布を示している。分布０６０１は、信頼度距離ｄの地点に対応する出現頻度分布が大きなほど、出現しやすい信頼度距離dの値であることを示している。

【００６８】

分布６０２、分布６０３は、それぞれ１、０のビット情報を埋め込んだデータから計算される信頼度距離ｄの分布を示している。同様に信頼度距離分布６０２、６０３でも同様に信頼度距離ｄの地点に対応する出現頻度分布が大きいほど、出現しやすい信頼度距離ｄの値であることを示している。なお、一つの信頼度距離ｄは一つのビット情報に対応している。

【００６９】

ここで、図６の６０１、６０２、６０３は、全て正規分布になっている。その理由を中心極限定理を用いて説明する。

【００７０】

＜中心極限定理＞

平均値m_c、標準偏差σ_cの母集団（正規分布でなくても良い）から大きさn_cの任意標本を抽出した時、標本平均値S_cの分布はn_cが大きくなるにつれて正規分布$N(mc,(s_c/\sqrt{n_c})^2)$に近づくことを示す定理である。

【００７１】

一般には母集団の標準偏差σ_cは不明なことが多いが、サンプル数n_cが十分大きく、母集団の数N_cがサンプル数n_cに比べてさらに十分大きいときは標本の標準偏差S_cをσ_cの代わりに用いても実用上ほとんど差し支えない。

【００７２】

本実施の形態において、部分集合Ａ，Ｂは夫々$A=\{a_1,a_2,..,a_N\}$、$B=\{b_1,b_2,...,b_N\}$で表されるＮ個の要素からなる集合で、夫々図５に示される様な部分集合Ａと部分集合Ｂの要素の持つ画素値とする。信頼度距離d（$\Sigma(a_i-b_i)/N$）は、Ｎが十分大きな値を取り、画素値a_iとb_iには相関がない場合は、信頼度距離ｄの期待値は０になる。また中心極限定理から、信頼度距離ｄの分布は正規分布をとることが分かる。

【００７３】

従って、信頼度距離ｄから埋め込まれたビット情報を判断する場合に、０と信頼度距離２ｃの間に適当な閾値を導入し、信頼度距離の絶対値が、閾値よりも大きい場合に埋め込みがあると判断することで、統計的に十分信頼できる情報の抽出が可能になる。

【００７４】

例えば、正規分布６０１の標準偏差をσとすると、付加情報の埋め込みがない場合には、図６の斜線部分で示す-1.96σ～$+1.96\sigma$の区間（９５％の信頼区間）に信頼度距離dは９５％の確率で出現する。

【００７５】

従って、閾値の値を大きくすると、閾値の外に出現する信頼度距離ｄの確率は

低くなり、信頼性の高い情報の抽出が可能になる。

【００７６】

また、埋め込み深さ「ｃ」を大きくすると、正規分布６０２、６０３はから遠ざかり、閾値を大きくすることも可能になる。

【００７７】

また部分集合ＡとＢの要素数Ｎを大きくすると、正規分布６０１、６０２、６０３の標準偏差σが小さくなるため、同じ埋め込み深さｃでも、より信頼性が高くなる。

【００７８】

以上がパッチワーク法の基本的な考え方である。

【００７９】

本実施の形態では、電子透かし埋め込み部２０４、電子透かし抽出部３０２は、以上で説明したパッチワーク法を用いている。

【００８０】

以下、電子透かしの埋め込み、抽出、除去の具体的な方法を説明する。

【００８１】

＜埋め込み位置決定部＞

パッチワーク法では、複数ビットからなる付加情報を埋め込むため、１つのビット情報ごとに部分集合ＡとＢが必要になる。従って、複数のビット情報を埋め込む場合には、ＡとＢ、Ａ’とＢ’、Ａ’’とＢ’’、…の位置を決定する必要がある。

【００８２】

図４の埋め込み位置決定部４０１では、複数のビットを埋め込むのに必要な埋め込み位置を決定する。埋め込み位置の決定方法としては、簡単なものとしては乱数を用いて決める方法が考えられる。各部分集合の要素がほぼ等しくなるようにし、部分集合がお互いに重なりあわず、画像全体にバランスよく埋め込まれることが好ましい。

【００８３】

一例として、画像と同じ大きさを有するホワイトノイズマスクを利用する方法

について簡単に述べる。

【００８４】

ホワイトノイズマスクは２次元的にマスク画素が配置され、それぞれのマスク画素は０～２５５の係数を持つ。ホワイトノイズマスクの０～２５５の各々の係数には、それぞれ略等しい数のマスク画素が割り当てられる。

【００８５】

例えば、原画像が２０００×２０００画素（＝４０００００画素）である場合、ホワイトノイズマスクのマスク画素も同じだけ用意することになるので、例えば０の値を持つマスク画素は、４０００００／２５６＝１５６２５個存在することになる。他の値を持つマスク画素も同じである。これらのマスク画素が乱数的に散りばめられたものをホワイトノイズマスクとするのである。

【００８６】

従って、１ビットの付加情報を埋め込む場合には、奇数の値を持つマスク画素を部分集合Ａに割り当て、偶数の階調を持つマスク画素を部分集合Ｂに割り当てると、部分集合Ａと部分集合Ｂの要素が等しく、重なり合わず、画像全体にバランスよく埋め込むことが可能になる。

【００８７】

Ｍ個からなる複数のビットの情報を埋め込む場合には、各ビットあたりに割り当てる画素の数を、１～Ｍのビット情報あたりに等しく割り当てる（例えば、ホワイトノイズマスクの取り得る範囲を２Ｍで割り、その剰余を部分集合ＡまたはＢに用いるなどして均等に割り当てる）ことにより、複数のビット情報の埋め込みが可能になる。

【００８８】

画素が８ビットで表される場合、階調数は２５６となるので、埋め込み可能な最大ビット数Ｍは１２８となる。ハッシュ値（６４ビットとか１２８ビット）のみの場合には、これで十分であるが、例えば、それ以外の情報（例えば著作権保護のための情報）を追加しようとすると足りなくなる場合がある。しかし、原画像を４分割し、それぞれの分割ブロックについて、それぞれのホワイトノイズマスクを設定すれば、１２８×４＝５１２ビットを埋め込むことが可能となる。ま

た、４分割ではなく、それ以上にすれば埋め込みビット数を増やすことも可能である。ただし、分割数を多くすると、逆に、正規分布になりずらくなるので、埋め込み情報の抽出が失敗することも有り得る。従って、原画像のサイズに応じて分割数を決定するようにすればよい。

【００８９】

従って、埋め込み位置決定部は、例えば予め用意されたマスクパターンを発生するだけで良いことになる。なお、電子透かしの抽出分離する側では、埋め込みで用いたマスクと同じものを用意しておき、これを利用することになる。

【００９０】

＜付加情報埋め込み部＞

付加情報埋め込み部４０２には、先に説明したように、画像データＩおよび、付加情報Ｅｓ（Ｈ）、埋め込み位置決定部４０１で決定された各ビットに対応する埋め込み位置が入力される。

【００９１】

入力される付加情報Ｅｓ（Ｈ）を構成するビット情報に従って各ビットに対応する部分集合ＡとＢの画素の画素値を操作する。

【００９２】

上述のパッチワーク法の説明で述べたように、ビット情報が１の場合には、部分集合Ａの画素の画素値に「ｃ」を加え、部分集合Ｂの画素の画素値から「ｃ」を減じる。ビット情報が０の場合には、部分集合Ａの画素の画素値から「ｃ」を減じ、部分集合Ｂの画素の画素値に「ｃ」を加えることになる。付加情報埋め込み部４０２では、以上の操作により、付加情報Ｅｓ（Ｈ）の埋め込みを行う。

【００９３】

以上説明した方法で付加情報の埋め込みを行うことが可能であるが、前記方法を実行した場合、ｃ＞a_iまたは、a_i＞２５５－ｃ、及び、ｃ＞b_iまたは、b_i＞２５５－ｃとなる画素においては、埋め込み後の画素値a_i'、及びb_i'が、a_i'、b_i'＜０、或いは、ａｉ’，ｂｉ’＞２５５となる。すると、後述する電子透かし除去部において、これらの画素については原画像の画素（即ち、ａｉ及びＢｉ）を復元することが出来ない。

【００９４】

よって本実施の形態においては、$c \leqq a_i \leqq 255-c$、及び$c \leqq b_i \leqq 255-c$となる画素に埋め込み処理を実行し、この範囲外の画素値に対しては埋め込み処理を行わない。従って、先にＭビットを埋め込む場合、先に「ホワイトノイズマスクの取り得る範囲を２Ｍで割り」と説明したが、この範囲を除外する必要がある。なお、これらの埋め込み処理を実行しない画素の位置情報をオーバーフロー位置情報として出力し、後述する電子透かし抽出部、及び電子透かし除去部に入力する必要がある。

【００９５】

＜電子透かし抽出手段＞

次に、本実施形態における電子透かし抽出部３０２について説明する。電子透かし抽出部３０２は、例えば、図７に示す構成になっている。

【００９６】

図示の様に、電子透かし抽出部３０２は、埋め込み位置決定部７０１、付加情報抽出部７０２、統計検定部７０３、比較部７０４、付加情報除去部７０５から構成される。

【００９７】

はじめに、電子透かし抽出部に、電子透かし埋め込みデータｗＩ’が入力される。次に埋め込み位置決定部７０１では、電子透かしが埋め込まれている位置情報（電子透かし埋め込み部２０４で使用したホワイトノイズマスクと同じパターン）を発生する。次の付加情報抽出部７０２では、入力される電子透かしが埋め込まれている位置情報を基に、電子透かし埋め込みデータに対し、所定の処理を施こすことによって、画像データｗＩ’に埋め込まれている付加情報Ｅ’ｓ（Ｈ）に対応する信頼度距離ｄを計算する。次の統計検定部７０３では、付加情報抽出部７０２で計算された付加情報Ｅ’ｓ（Ｈ）に対応するデータの確からしさを、統計的に検定する。充分正確な付加情報Ｅ’ｓ（Ｈ）であると判定された場合には、比較部７０４により付加情報Ｅｓ（Ｈ）の抽出を行う。確からしくなければ情報なしと出力する。情報が埋め込まれている場合には、入力された画像データｗＩ’，埋め込み位置決定部７０２からの埋め込み位置情報、及びオーバーフロ

ー位置情報を用いて、付加情報除去部７０５において電子透かしが除去される。

【００９８】

次に、電子透かしが埋め込まれた画像データｗＩ’からこの付加情報Ｅ’ｓ（Ｈ）を抽出する電子透かし抽出部の動作について詳細に述べる。

【００９９】

＜埋め込み位置決定部＞

埋め込み位置決定部７０１において、画像データｗＩ’中のどの領域から付加情報Ｅ’ｓ（Ｈ）を抽出するかを決定する。この埋め込み位置決定部７０１によってなされる動作は、前述した埋め込み位置決定部４０１と同じであり、その為、４０１と８０１によって決定される埋め込み位置は同一のものとなる。決定された埋め込み位置の情報は、付加情報抽出部７０２、及び付加情報除去部７０５に出力される。

【０１００】

＜付加情報抽出部＞

付加情報抽出部７０２では、埋め込み位置決定部７０１で決定された埋め込み位置から各ビットに対応する信頼度距離ｄを計算する。この際に、入力されたオーバーフロー位置情報に従い、ここに示されている画素には付加情報は埋め込まれていないため、信頼度距離ｄの算出には用いない。

【０１０１】

＜統計検定部＞

統計検定部７０３では、付加情報抽出部７０２から出力されるそれぞれのビット情報に対応する信頼度距離ｄに対して、確からしさを統計的に検定する。複数ビットの情報を埋め込んでいる場合には、複数の信頼度距離ｄが得られる。付加情報Ｅ’ｓ（Ｈ）が埋め込まれている場合には、信頼度距離ｄは図６では、中心０から離れた位置２ｃを中心とした位置に出現する。

【０１０２】

このとき、埋め込み深さｃが大きければ大きいほど、信頼度距離ｄは図６において、中心０から離れて出現する。従って、「ｃ」の位置に閾値を導入し、「ｃ」よりも大きな信頼度距離ｄが得られる場合には、埋め込まれたビット情報は１

であり、－ｃよりも小さな信頼度距離dが得られる場合には埋め込まれたビット情報は０であると判断できる。

【０１０３】

従って、付加情報の埋め込み時に埋め込み深さ「ｃ」が大きければ大きいほど、正規分布６０１、６０２および６０３の間隔が広がり、抽出情報の信頼性が高くなる。また部分集合ＡおよびＢの要素数Ｎが大きければ大きいほど、正規分布６０１、６０２および６０３の標準偏差は小さくなる。従って、埋め込み深さ「ｃ」および部分集合ＡおよびＢの要素数Ｎを大きくすることで、閾値が「ｃ」の場合でも抽出情報の信頼が高く設定できる。

【０１０４】

なお、埋め込みがない場合の信頼度距離ｄは－ｃ～ｃの小さな区間に全て出現する（しやすい）ので、それを利用して判断する。

【０１０５】

すなわち、本実施形態の統計検定部７０３では、複数のビットに対応する信頼度距離ｄがある一定以上、－ｃ～ｃの範囲に出現する場合には、情報が埋め込まれていないと判断し、その旨を表示する。

【０１０６】

＜比較部＞

図７の比較部７０４には、付加情報抽出部７０２と統計検定部７０３を経て出力された各ビット情報に対応する信頼度距離ｄの値が供給される。

【０１０７】

比較部７０４に入力される各ビット情報に対応する信頼度距離ｄは信頼性の高い情報であるので、各ビット情報に対応する信頼度距離ｄの正または負の符号から、“１”または“０”の何れであるかを単純に判定するだけで良い。

【０１０８】

具体的には、付加情報Ｅ’ｓ（Ｈ）を構成するあるビット情報の信頼度距離ｄが「ｃ」より大きい場合、このビット情報が“１”であると判定し、信頼度距離ｄが［－ｃ］より小さい場合はこのビット情報が“０”であると判定する。

【０１０９】

＜付加情報除去部＞

付加情報除去部７０５で行なわれる操作を説明する。付加情報除去部７０５には、付加情報Ｅ’ｓ（Ｈ）の埋め込み位置、画像データｗＩ’、及びオーバーフロー位置情報が入力され、付加情報が除去された画像データＩ’が出力される。

【０１１０】

電子透かし埋め込み部における付加情報埋め込み部４０２で行った埋め込みを行った位置と同一の位置で、各ビットに対応する部分集合に対し、埋め込み深さｃを埋め込み時とは符号を反対にして加えることで、付加情報を除去し、原画像を復元する。

【０１１１】

具体的には、付加情報Ｅ’ｓ（Ｈ）を構成する所定のビット情報の埋め込み位置において、ビット情報が１である場合、

$a'_i = a_i - c$

$b'_i = b_i + c$

の処理を行い、ビット情報が０の場合には、

$a'_i = a_i + c$

$b'_i = b_i - c$

の処理を行うことで、それぞれ埋め込み前の画素値に復元することが可能になる。この際に、入力されたオーバーフロー位置情報に従う。従ってオーバーフロー位置である画素には付加情報は埋め込まれていないため、除去の対象にはしない。

【０１１２】

以上で述べた操作を行い、付加情報除去部７０５は、電子透かし埋め込みデータｗＩ’から電子透かしを除去し、電子透かしが除去された画像データＩ’を出力する。

【０１１３】

以上の実施形態においては、認証情報としてディジタル署名を用いる方法について説明したが、本発明はこれに限定されることなく、例えば認証情報としてＭＡＣ（メッセージ認証符号）を用いる方法も含まれることも明らかである。更に

、ディジタル署名、或いは、ＭＡＣに加えて、日付情報、位置情報、時間情報、装置の固有情報、署名者の固有情報のうち少なくとも一つ以上を含むことも可能である。

【０１１４】

更に、以上の実施の形態において、付加情報には誤り訂正符号化されたものを用いることも可能であり、そうする事によって、更に抽出された付加情報Infの信頼性を向上させることができる。

【０１１５】

なお、上述した情報を埋め込む側、及び、埋め込まれた情報を認証する側の装置は、そのほとんどがソフトウェアでもって実現できる。すなわち、図２、図３に示す各処理部はソフトウェアで構成できる。

【０１１６】

この場合、装置構成は、一般のパーソナルコンピュータ等の汎用装置で良く、その一例を示せば図１の構成とすることができる。

【０１１７】

同図は本実施の形態に適用する画像処理装置の全体構成を示したものである。本図において、ホストコンピュータ１０１は例えば一般に普及しているパーソナルコンピュータである。

【０１１８】

ホストコンピュータ１０１の内部では、バス１０７により後述する各ブロックが接続され、種々のデータの受け渡しが可能である。

【０１１９】

図中、１０３は、内部の各ブロックの動作を制御、或いは内部に記憶されたプログラムを実行することのできるＣＰＵである。１０４は、ブートプログラムやＢＩＯＳを記憶しているＲＯＭである。１０５はＣＰＵにて処理を行うために一時的にプログラムや処理対象の画像データを格納しておくＲＡＭである。１０６は、ＲＡＭ等に転送されるプログラム（ＯＳや画像処理プログラム）や画像データをあらかじめ格納したり、処理後の画像データを保存することのできるハードディスク（ＨＤ）である。著名装置として機能する場合には、このハードディス

ク１０６には、図２に対応するプログラムが格納され、ＲＡＭ１０５にロードされ実行されることになる。また、認証装置として機能する場合には、図３に示す構成に対応するプログラムがこのハードディスク１０６に格納され、ＲＡＭ１０５にロードされ実行されることになる。

【０１２０】

１０８は、外部記憶媒体の一つであるＣＤ（ＣＤ－Ｒ）に記憶されたデータを読み込み或いは書き出すことのできるＣＤドライブである。１０９は、１０８と同様にＦＤからの読み込み、ＦＤへの書き出しができるＦＤドライブである。１１０も、１０８と同様にＤＶＤからの読み込み、ＤＶＤへの書き出しができるＤＶＤドライブである。尚、ＣＤ，ＦＤ，ＤＶＤ等に画像編集用のプログラム、或いはプリンタドライバが記憶されている場合には、これらプログラムをＨＤ１０６上にインストールし、必要に応じてＲＡＭ１０５に転送されるようになっている。これらの記憶媒体は、オリジナル画像を記憶させ、それに著名情報を埋め込むことに使用されたり、逆に、配布された記憶媒体内の著名付き画像について認証処理を行うことになる。

【０１２１】

１１３は、キーボード１１１或いはマウス１１２からの入力指示を受け付けるためにこれらと接続されるインターフェイス（Ｉ／Ｆ）である。また、１１４はグラフィックコントローラ及びビデオメモリ（不図示）を内蔵し、表示に関する制御を行う表示制御部であり、ビデオメモリに展開されたイメージデータを表示装置１１５に出力することで像を表示させる。１１５は通信インタフェースであり、インターネットに接続するためのものである（例えば、モデムやイーサネットボード等）。著名情報を付加した情報をこの通信インタフェース１１５で送信したり、或いは受信することも可能となる。

【０１２２】

なお、イメージデータを入力する手段として、上記に限らず、イメージスキャナ等でも構わないのは勿論である。

【０１２３】

以上のように、本発明は、複数の機器（例えばホストコンピュータ、インタフ

ェース機器、リーダ、プリンタ等）から構成されるシステムの１部として適用しても、１つの機器（例えば携帯端末やＰＤＡ等）からなるものの１部に適用してもよい。

【０１２４】

また、本発明は上記の如く、システム又は装置内のコンピュータ（CPUあるいはＭＰＵ）に、上記実施の形態を実現する為のソフトウエアのプログラムコードを供給し、このプログラムコードに従って上記システムあるいは装置のコンピュータが上記各種デバイスを動作させることにより上記実施の形態を実現する場合も本発明の範疇に含まれる。

【０１２５】

またこの場合、前記ソフトウエアのプログラムコード自体が上記実施の形態の機能を実現することになり、そのプログラムコード自体、及びそのプログラムコードをコンピュータに供給する為の手段、具体的には上記プログラムコードを格納した記憶媒体は本発明の範疇に含まれる。

【０１２６】

この様なプログラムコードを格納する記憶媒体としては、例えばフロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ等を用いることができる。

【０１２７】

また、上記コンピュータが、供給されたプログラムコードのみに従って各種デバイスを制御することにより、上記実施の形態の機能が実現される場合だけではなく、上記プログラムコードがコンピュータ上で稼働しているＯＳ（オペレーティングシステム）、あるいは他のアプリケーションソフト等と共同して上記実施の形態が実現される場合にもかかるプログラムコードは本発明の範疇に含まれる。

【０１２８】

更に、この供給されたプログラムコードが、コンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能格納ユニットに

備わるCPU等が実際の処理の一部又は全部を行い、その処理によって上記実施の形態が実現される場合も本発明の範疇に含まれる。

【０１２９】

以上説明した様に本実施形態によれば、ディジタル情報と署名情報を不可分の状態とすることが可能であり、フォーマット変換などを介しても署名情報を認証装置に送信することが可能となる。

【０１３０】

【発明の効果】

以上説明したように本発明によれば、認証情報をディジタル情報と不可分にししつつ、改ざんがなされているか否かを判断でき、しかも改ざんがない限りはオリジナルのディジタル情報に復元することが可能になる。

【図面の簡単な説明】

【図１】

実施形態で適用可能なコンピュータのブロック構成図である。

【図２】

実施形態における署名装置のブロック構成図である。

【図３】

実施形態における認証装置のブロック構成図である。

【図４】

図２における電子透かし埋め込み部の詳細を示す図である。

【図５】

パッチワーク法の原理を説明するための図である。

【図６】

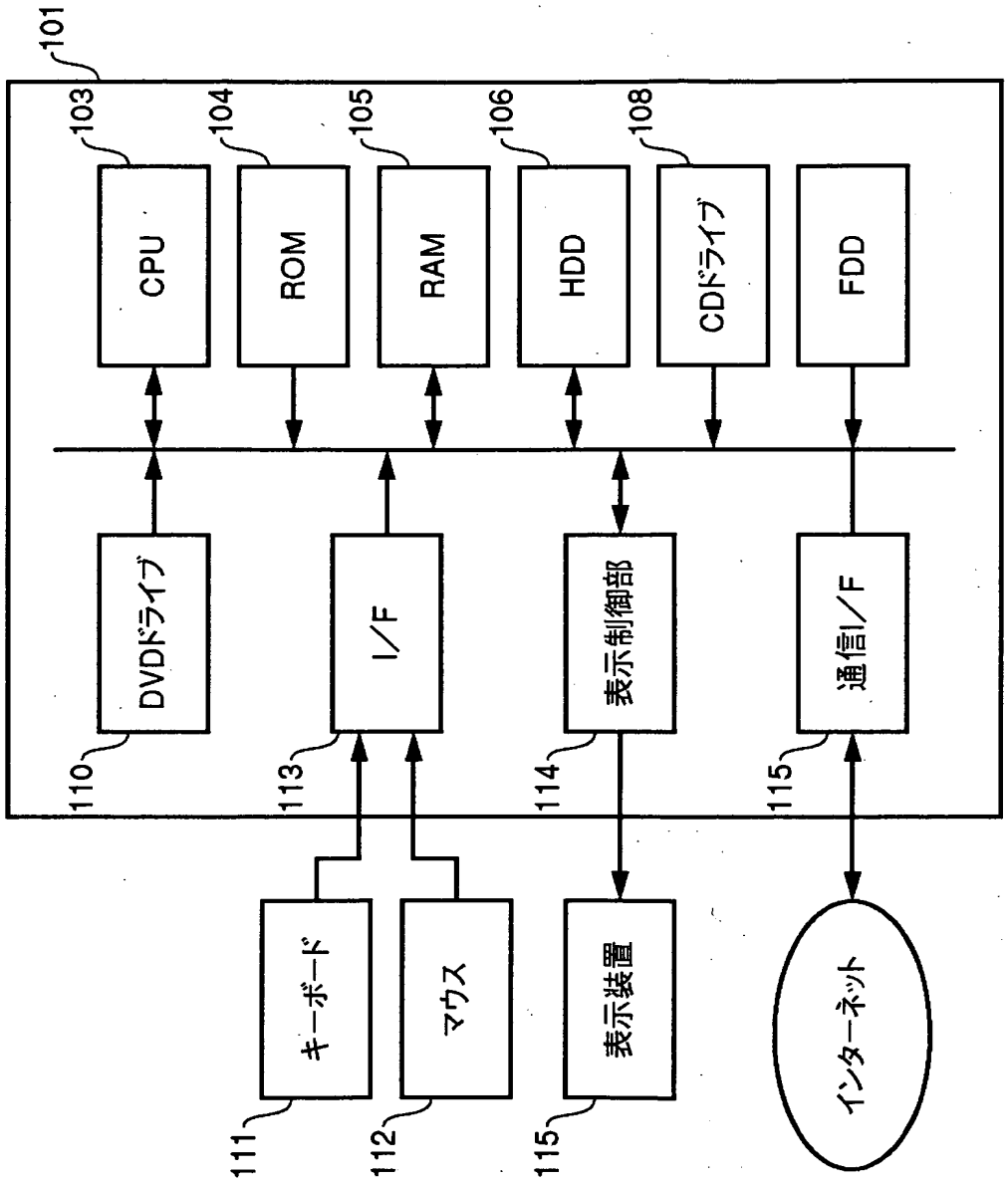
電子透かし抽出時の信頼度距離ｄの出現頻度分布を示す図である。

【図７】

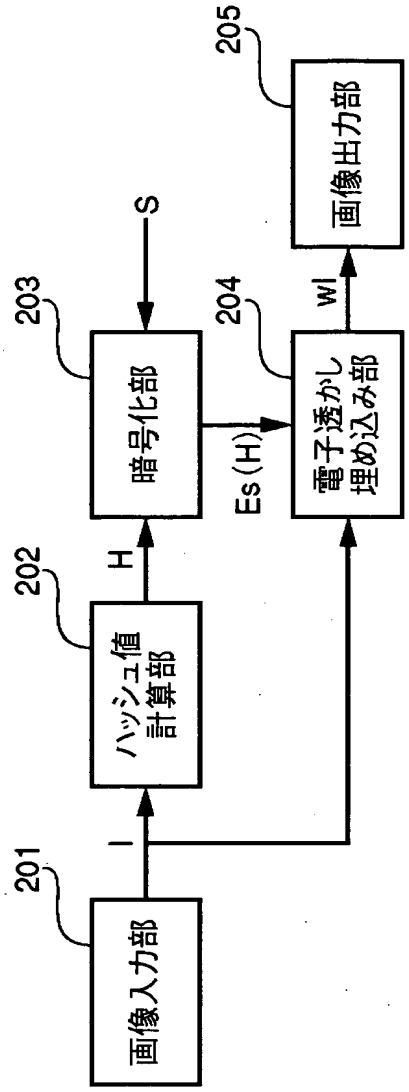
実施形態における電子透かし抽出部のブロック構成図である。

【書類名】　　図面

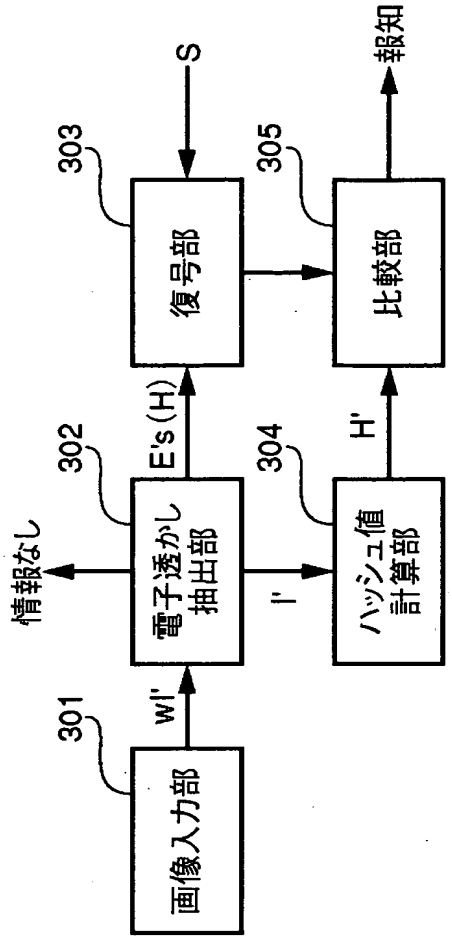
【図１】


101
103
104
105
106
108
CPU
ROM
RAM
HDD
CDドライブ
FDD
DVDドライブ
I／F
表示制御部
通信I／F
110
113
114
115
キーボード
マウス
表示装置
インターネット
111
112
115

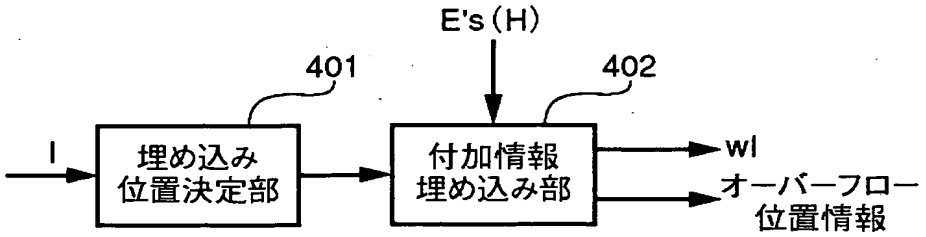
【図２】


205
画像出力部
S
203
暗号化部
204
電子透かし
埋め込み部
wI
Es(H)
202
ハッシュ値
計算部
H
I
201
画像入力部

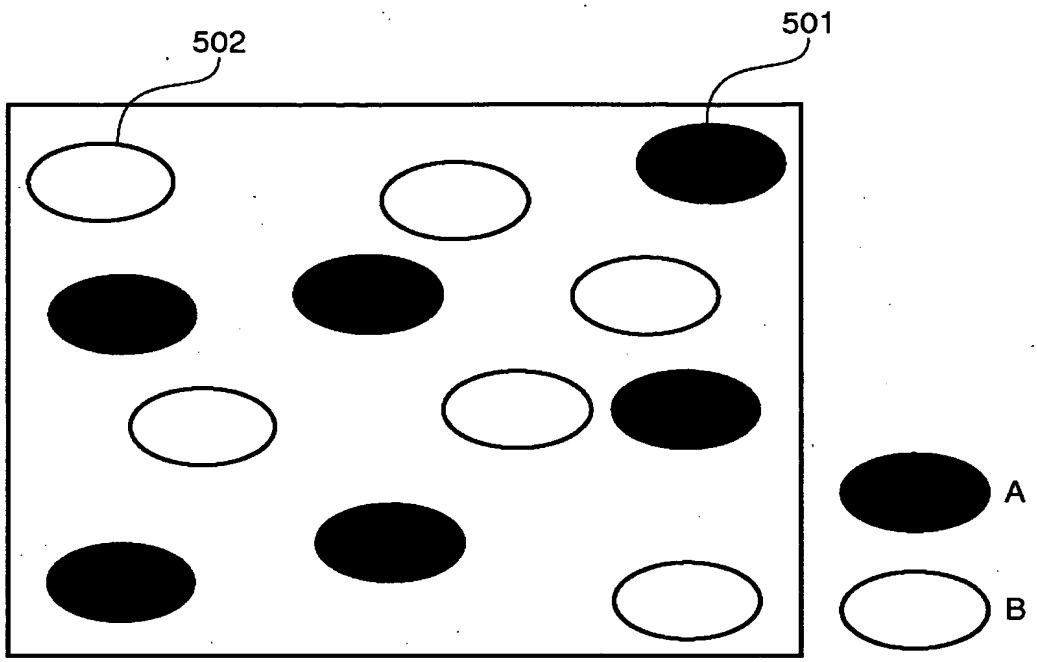
【図３】


S
報知
303
305
復号部
比較部
E's (H)
H'
302
304
情報なし
電子透かし
抽出部
ハッシュ値
計算部
I'
wI'
301
画像入力部

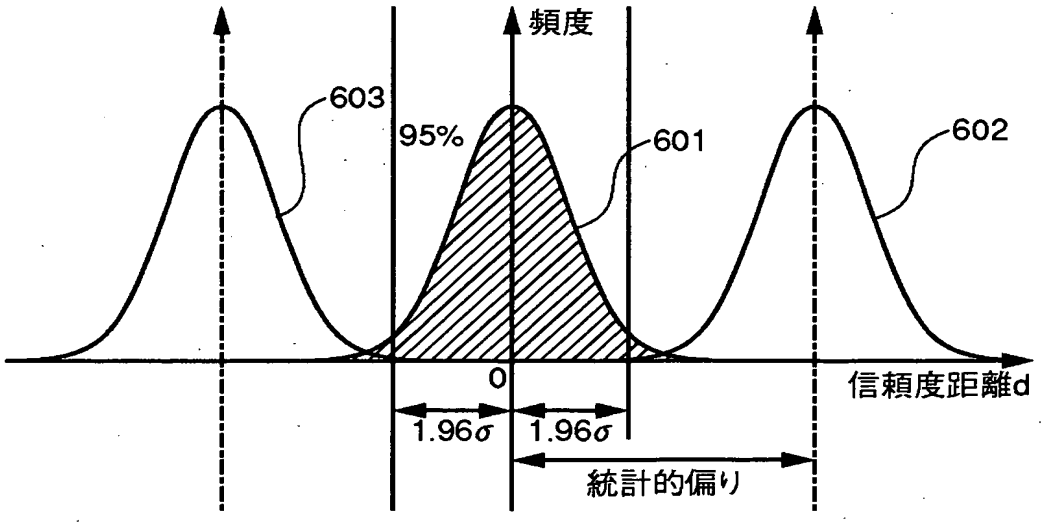
【図４】


E's (H)
401
402
I
埋め込み
位置決定部
付加情報
埋め込み部
wI
オーバーフロー
位置情報

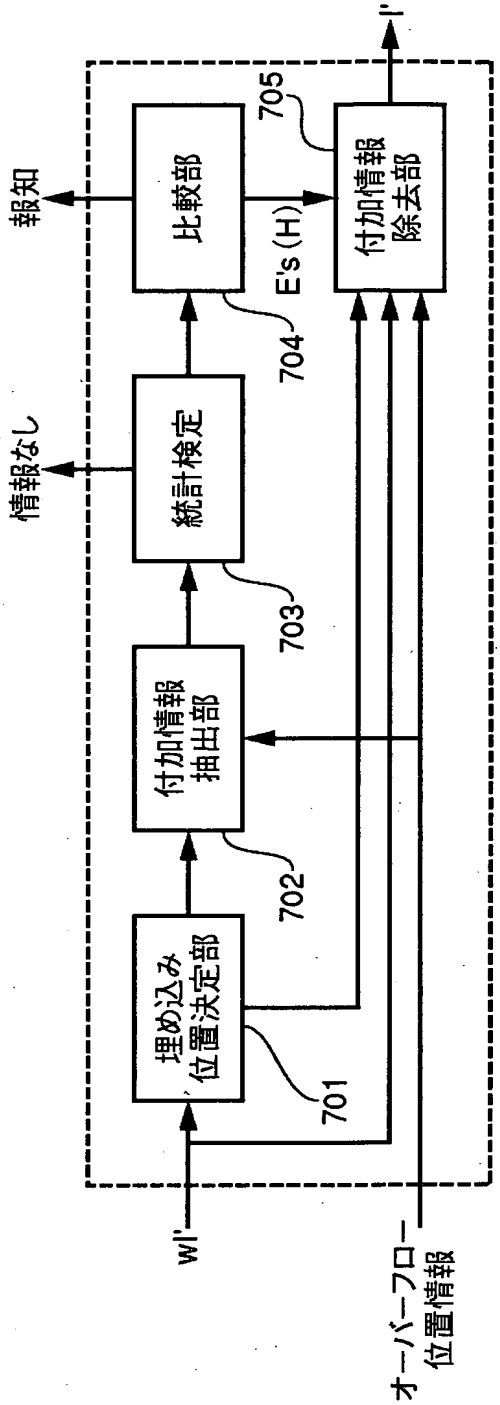
【図５】



【図６】



【図７】


w'
埋め込み位置決定部
701
702
付加情報抽出部
703
統計検定
704
比較部
705
付加情報除去部
w
情報なし
報知
E's (H)
オーバーフロー位置情報

【書類名】　要約書

【要約】

【課題】　認証情報をディジタル情報と不可分にししつつ、改ざんがなされているか否かを判断でき、しかも改ざんがない限りはオリジナルのディジタル情報に復元することを可能にする。

【解決手段】　画像入力部２０１より入力したディジタル情報に認証情報を埋め込む場合、そのディジタル情報に基づいてハッシュ値計算部２０２で認証情報を生成し、暗号化部２０３で暗号化鍵で暗号化し、電子透かし埋め込み部２０４で、それをディジタル情報に電子透かしとして埋め込む。

【選択図】　図２

出　願　人　履　歴　情　報

識別番号　　〔０００００１００７〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　　東京都大田区下丸子３丁目３０番２号
氏　名　　キヤノン株式会社